Senate File 203 - Introduced

SENATE FILE 203
BY COMMITTEE ON TECHNOLOGY

(SUCCESSOR TO SSB 1072)

A BILL FOR

- 1 An Act relating to ransomware and providing penalties.
- 2 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

- 1 Section 1. Section 715.2, Code 2023, is amended to read as 2 follows:
- 3 715.2 Title.
- 4 This chapter shall be known and may be cited as the "Computer
- 5 Spyware, Malware, and Ransomware Protection Act".
- 6 Sec. 2. Section 715.3, Code 2023, is amended by adding the
- 7 following new subsections:
- 8 NEW SUBSECTION. 1A. "Computer control language" means
- 9 ordered statements that direct a computer to perform specific
- 10 functions.
- 11 NEW SUBSECTION. 1B. "Computer database" means a
- 12 representation of information, knowledge, facts, concepts, or
- 13 instructions that is intended for use in a computer, computer
- 14 system, or computer network that is being prepared or has been
- 15 prepared in a formalized manner, or is being produced or has
- 16 been produced by a computer, computer system, or computer
- 17 network.
- 18 NEW SUBSECTION. 9A. "Ransomware" means a computer or data
- 19 contaminant, encryption, or lock that is placed or introduced
- 20 without authorization into a computer, computer network, or
- 21 computer system that restricts access by an authorized person
- 22 to a computer, computer data, a computer system, or a computer
- 23 network in a manner that results in the person responsible for
- 24 the placement or introduction of the contaminant, encryption,
- 25 or lock making a demand for payment of money or other
- 26 consideration to remove the contaminant, encryption, or lock.
- 27 Sec. 3. Section 715.5, subsection 2, Code 2023, is amended
- 28 to read as follows:
- 29 2. Using intentionally deceptive means to cause the
- 30 execution of a computer software component with the intent of
- 31 causing an owner or operator to use such component in a manner
- 32 that violates any other provision of this chapter subchapter.
- 33 Sec. 4. Section 715.6, Code 2023, is amended to read as
- 34 follows:
- 35 715.6 Exceptions.

- 1 Sections 715.4 and 715.5 shall not apply to the following:
- 2 1. The monitoring of, or interaction with, an owner's or
- 3 an operator's internet or other network connection, service,
- 4 or computer, by a telecommunications carrier, cable operator,
- 5 computer hardware or software provider, or provider of
- 6 information service or interactive computer service for network
- 7 or computer security purposes, diagnostics, technical support,
- 8 maintenance, repair, authorized updates of computer software
- 9 or system firmware, authorized remote system management, or
- 10 detection, criminal investigation, or prevention of the use of
- ll or fraudulent or other illegal activities prohibited in this
- 12 chapter in connection with a network, service, or computer
- 13 software, including scanning for and removing computer software
- 14 prescribed under this chapter subchapter. Nothing in this
- 15 chapter subchapter shall limit the rights of providers of wire
- 16 and electronic communications under 18 U.S.C. §2511.
- 17 2. The nonpayment or a violation of the terms of a legal
- 18 contract with the owner or operator.
- 19 3. For complying with federal, state, and local law
- 20 enforcement requests.
- 21 Sec. 5. Section 715.7, Code 2023, is amended to read as
- 22 follows:
- 23 715.7 Criminal penalties.
- 24 1. A person who commits an unlawful act under this chapter
- 25 <u>subchapter</u> is guilty of an aggravated misdemeanor.
- 26 2. A person who commits an unlawful act under this chapter
- 27 subchapter and who causes pecuniary losses exceeding one
- 28 thousand dollars to a victim of the unlawful act is quilty of a
- 29 class "D" felony.
- 30 Sec. 6. Section 715.8, unnumbered paragraph 1, Code 2023,
- 31 is amended to read as follows:
- 32 For the purpose of determining proper venue, a violation
- 33 of this chapter subchapter shall be considered to have been
- 34 committed in any county in which any of the following apply:
- 35 Sec. 7. NEW SECTION. 715.9 Ransomware prohibition.

- 2 authorization do any of the following:
- 3 a. Access, attempt to access, cause to be accessed, or
- 4 exceed the person's authorized access to all or a part of a
- 5 computer network, computer control language, computer, computer
- 6 software, computer system, or computer database.
- 7 b. Copy, attempt to copy, possess, or attempt to possess
- 8 the contents of all or part of a computer database accessed in
- 9 violation of paragraph "a".
- 2. A person shall not commit an act prohibited in subsection
- 11 1 with the intent to do any of the following:
- 12 a. Cause the malfunction or interruption of the operation
- 13 of all or any part of a computer, computer network, computer
- 14 control language, computer software, computer system, computer
- 15 service, or computer data.
- 16 b. Alter, damage, or destroy all or any part of data or a
- 17 computer program stored, maintained, or produced by a computer,
- 18 computer network, computer software, computer system, computer
- 19 service, or computer database.
- A person shall not intentionally, willfully, and without
- 21 authorization do any of the following:
- 22 a. Possess, identify, or attempt to identify a valid
- 23 computer access code.
- 24 b. Publicize or distribute a valid computer access code to
- 25 an unauthorized person.
- 26 4. A person shall not commit an act prohibited under this
- 27 section with the intent to interrupt or impair the functioning
- 28 of any of the following:
- 29 a. The state.
- 30 b. A service, device, or system related to the production,
- 31 transmission, delivery, or storage of electricity or natural
- 32 gas in the state that is owned, operated, or controlled by a
- 33 person other than a public utility as defined in chapter 476.
- 34 c. A service provided in the state by a public utility as
- 35 defined in section 476.1, subsection 3.

- 1 d. A hospital or health care facility as defined in section 2 135C.1.
- 3 e. A public elementary or secondary school, community
- 4 college, or area education agency under the supervision of the
- 5 department of education.
- 6 f. A city, city utility, or city service.
- 7 g. An authority as defined in section 330A.2.
- 8 5. This section shall not apply to the use of ransomware for
- 9 research purposes by a person who has a bona fide scientific,
- 10 educational, governmental, testing, news, or other similar
- 11 justification for possessing ransomware. However, a person
- 12 shall not knowingly possess ransomware with the intent to
- 13 use the ransomware for the purpose of introduction into the
- 14 computer, computer network, or computer system of another
- 15 person without the authorization of the other person.
- 16 6. A person who has suffered a specific and direct injury
- 17 because of a violation of this section may bring a civil action
- 18 in a court of competent jurisdiction.
- 19 a. In an action under this subsection, the court may award
- 20 actual damages, reasonable attorney fees, and court costs.
- 21 b. A conviction for an offense under this section is not a
- 22 prerequisite for the filing of a civil action.
- 23 Sec. 8. NEW SECTION. 715.10 Criminal penalties.
- 24 l. A person who commits an unlawful act under this
- 25 subchapter and who causes pecuniary losses involving less than
- 26 ten thousand dollars to a victim of the unlawful act is guilty
- 27 of an aggravated misdemeanor.
- 28 2. A person who commits an unlawful act under this
- 29 subchapter and who causes pecuniary losses involving at least
- 30 ten thousand dollars but less than fifty thousand dollars to a
- 31 victim of the unlawful act is guilty of a class "D" felony.
- 32 3. A person who commits an unlawful act under this
- 33 subchapter and who causes pecuniary losses involving at least
- 34 fifty thousand dollars to a victim of the unlawful act is
- 35 quilty of a class "C" felony.

- 1 Sec. 9. NEW SECTION. 715.11 Venue.
- 2 For the purpose of determining proper venue, a violation of
- 3 this subchapter shall be considered to have been committed in
- 4 any county in which any of the following apply:
- 5 1. Where the defendant performed the unlawful act.
- 6 2. Where the defendant resides.
- Where the accessed computer is located.
- 8 Sec. 10. CODE EDITOR DIRECTIVE. The Code editor shall
- 9 divide chapter 715 into subchapters and shall designate
- 10 sections 715.1 through 715.3, including sections amended in
- 11 this Act, as subchapter I entitled "INTENT AND DEFINITIONS",
- 12 sections 715.4 through 715.8, including sections amended in
- 13 this Act, as subchapter II entitled "COMPUTER SPYWARE AND
- 14 MALWARE", and sections 715.9 through 715.11, as enacted in this
- 15 Act, as subchapter III entitled "RANSOMWARE".
- 16 EXPLANATION
- 17 The inclusion of this explanation does not constitute agreement with 18 the explanation's substance by the members of the general assembly.
- 19 This bill relates to ransomware.
- 20 The bill defines "ransomware" as a computer or data
- 21 contaminant, encryption, or lock that is placed or introduced
- 22 without authorization into a computer, computer network, or a
- 23 computer system that restricts access by an authorized person
- 24 to a computer, computer data, a computer network, or a computer
- 25 system in a manner that results in the person responsible for
- 26 the placement or introduction of the contaminant, encryption,
- 27 or lock making a demand for payment of money or other
- 28 consideration to remove the contaminant, encryption, or lock.
- 29 The bill provides that the monitoring of, or interaction
- 30 with, an owner's or operator's internet or other network
- 31 connection, service, or computer is not prohibited for support
- 32 or maintenance, the investigation of illegal activities, the

-5-

- 33 nonpayment or violation of the terms of a contract, or for
- 34 complying with federal, state, and local law enforcement
- 35 requests.

```
1
      The bill provides that a person shall not do any of
 2 the following with the intent to cause the malfunction or
 3 interruption of the operation of, or alter, damage, or destroy,
 4 all or any part of a computer, computer network, computer
 5 control language, computer software, computer system, computer
 6 service, or computer data: intentionally, willfully, and
 7 without authorization access, attempt to access, cause to be
8 accessed, or exceed the person's authorized access to all
 9 or a part of a computer network, computer control language,
10 computer, computer software, computer system, or computer
11 database; or copy, attempt to copy, possess, or attempt to
12 possess the contents of all or part of a computer database.
13
      The bill provides that a person shall not intentionally,
14 willfully, and without authorization possess, identify,
15 or attempt to identify a valid access code or publicize or
16 distribute a valid access code to an unauthorized person.
17
      The bill provides that a person shall not commit a prohibited
18 act with the intent to interrupt or impair the functioning of
19 the state government; a service, device, or system related
20 to the production, transmission, delivery, or storage of
21 electricity or natural gas in the state that is owned,
22 operated, or controlled by a person other than a public utility
23 as defined in Code section 476.1(3); a service provided in
24 the state by a public utility as defined in Code chapter 476;
25 a hospital or health care facility; a public elementary or
26 secondary school, community college, or area education agency
27 under the supervision of the department of education; a city,
28 city utility, or city service; or an aviation authority.
29
      The bill does not apply to the use of ransomware for
30 research purposes by a person who has a bona fide scientific,
31 educational, governmental, testing, news, or other similar
32 justification for possessing ransomware. However, a person
33 shall not knowingly possess ransomware with the intent to
34 use the ransomware for the purpose of introduction into the
35 computer, computer network, or computer system of another
```

as/rh

- 1 person without the authorization of the other person.
- 2 The bill provides that a person who has suffered a specific
- 3 and direct injury because of a violation of the bill may bring
- 4 a civil action in a court of competent jurisdiction, and the
- 5 court may award actual damages, reasonable attorney fees, and
- 6 court costs. A conviction for an offense under the bill is not
- 7 a prerequisite for the filing of a civil action.
- 8 The bill provides that a person who commits a violation
- 9 of the bill and who causes pecuniary losses involving less
- 10 than \$10,000 to a victim of the unlawful act is guilty of an
- 11 aggravated misdemeanor. A person who commits a violation of
- 12 the bill and who causes pecuniary losses involving at least
- 13 \$10,000 but less than \$50,000 to a victim of the unlawful
- 14 act is guilty of a class "D" felony. A person who commits a
- 15 violation of the bill and who causes pecuniary losses involving
- 16 at least \$50,000 to a victim of the unlawful act is guilty of a
- 17 class "C" felony.
- An aggravated misdemeanor is punishable by confinement for
- 19 no more than two years and a fine of at least \$855 but not more
- 20 than \$8,540. A class "D" felony is punishable by confinement
- 21 for no more than five years and a fine of at least \$1,025 but
- 22 not more than \$10,245. A class "C" felony is punishable by
- 23 confinement for no more than 10 years and a fine of at least
- 24 \$1,370 but not more than \$13,660.
- 25 The bill provides that for the purpose of determining
- 26 venue, a violation of the bill shall be considered to have
- 27 been committed in any county where the defendant performed
- 28 the unlawful act, where the defendant resides, or where the
- 29 accessed computer is located.